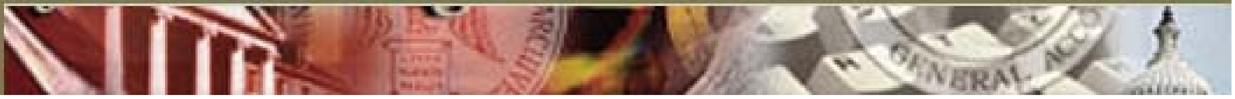
PRIVACY AWARENESS



Safeguarding Data

While personal information is being collected, stored, used or disclosed for National Institutes (NIH) purposes, it must be protected from unauthorized access. The Privacy Act of 1974, as amended, states that administrative, technical and physical safeguards must be implemented throughout the life cycle of personal information.

To be in compliance with the Privacy Act, NIH must:

- Collect information directly from an individual to the greatest extent possible;
- Establish appropriate administrative, technical and physical safeguards to ensure security and confidentiality; and,
- Conduct a risk analysis every three years (initiated by system managers).

Administrative Safeguards

Here are some examples of administrative or procedural safeguards you should put into place:

- Policies and Guides;
- User Manuals;
- Privacy Impact Assessments (PIAs);
- Certification & Accreditation (C&A) Programs;
- Back-up File Storage; and,
- Contingency Plans.

Technical Safeguards

Here are the NIH required technical safeguards for electronic data:

- Passwords (mandatory);
- Encryption (for stored and transmitted data); and
- 30-Minute Timeout Policy (for VPN connections and mobile devices)

Here are some examples of minimal standards of technical safeguards which you should implement:

- User IDs;
- Firewalls;
- Cryptology;
- Virtual Private Networks;
- Intrusion Protection;
- Common Access Cards;

- Smart Cards;
- Biometrics; and
- Public Key Infrastructure

Here is a list of technical safeguards you should implement at your desk:

- Log out of or lock your computer;
- Put a password protected screensaver on your computer;
- Keep personal information in folders or turn papers upside down if you are going to leave the office of a short period of time;
- Lock your files when you leave;
- Before disposing of documents, shred those that contain personal information;
- Keep passwords and keys in a safe place;
- Label files with privacy in mind;
- Shut down your computer when you leave work at the end of the day; and
- Follow IT security rules when using the internet, fax and e-mail

Physical Security Access Control Safeguards

NIH must implement physical safeguards as well. These include, but are not limited to:

- Protection against fire, structural collapse, plumbing leaks;
- Post a security guard in the lobby of the building;
- Use a sign-in/sign-out log for visitors to the building or office;
- Require employees to wear identification badges;
- Install a closed-circuit TV or CCTV;
- Use key cards, cipher locks or biometrics to access sensitive areas;
- Put locks on drawers, file cabinets, and doors;
- Limit key holders;
- Store files in a facility with limited access or alarms;
- Lock up equipment that holds data, such as laptops and computers;
- Post “Authorized Personnel Only” signs and/or “Privacy Warning” notices; and,
- Protect files while in transit.

NOTE:

NIH employees who telecommute or carry electronic data home place Privacy Act information in danger of being lost or stolen. Misplacing sensitive data places our employees, customers, patients, and business partners at risk for identity theft, credit card theft, or public exposure of personal information. It is your responsibility to apply safeguards to your remote computer, portable devices and/or home office.

Follow these guidelines to protect personally identifiable information (PII):

- Restrict access to personally identifiable information;
- Only provide the authority to access PII if that access is necessary for a business process;
- Don't keep personal information unless you need it to do your job;
- Keep sensitive paper records under lock and key and protect them;
- Don't include SSNs in reports or data collections unless the SSN is essential to the business process;
- Remove unnecessary personal information from any laptop or removable and portable disk storage device;
- Encrypt personal data that you must store and send;
- Encrypt the data on laptops. There's no good excuse for losing sensitive data when an encrypted laptop is lost or stolen. If you have a government-issued laptop that is not encrypted, contact your computer support and ask that it be protected with encryption;
- Clear out web browser sessions by deleting temporary files;
- Report security incidents, or suspected incidents, to your Information Systems Security Officer, or supervisor; and
- If you're a supervisor, you must ensure that all telework agreements address privacy, records management and security practices

NIH Information Technology General Rules of Behavior

NIH maintains a set of mandatory rules which summarize laws and guidelines from various NIH and other Federal documents, especially OMB Circular A-130 and Section 208 of the E-Government Act of 2002. These rules should be adhered to by all NIH personnel, contractors, visitors, and fellows. Anyone who connects to the NIH network is obligated to follow them.

The NIH IT Rules of Behavior were established to hold users accountable for their actions and to be responsible for information security. An essential part of your job is to take responsibility for the security of your computer and the data it contains. To view a complete list of the NIH IT Rules of Behavior, please refer to: http://irm.cit.nih.gov/security/nihitrob.html

As we have seen in too many cases, whether it be a stolen laptop, a misaddressed envelope, a file placed on a public web site, a computer system accessed by a hacker, a fax sent to a number that was inadvertently transposed, an e-mail that was sent unencrypted, these safeguards are only successful when NIH employees, contractors and those organizations with whom we collaborate, are aware of them, are trained to implement them, properly follow them, and revise them as new privacy and security threats arise.

Bottom-line: Any of the above events could put a person’s sensitive financial, personnel or medical information at risk. Do not let information that has been entrusted to NIH get into the wrong hands. If you have questions about protecting information in identifiable form, discuss the issue with your supervisor and contact your ISSO, your IC Privacy Coordinator, the NIH Chief Information Security Officer, or the NIH Senior Official for Privacy.